DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-3/5/7
400 ARMY PENTAGON
WASHINGTON, DC 20310-0400

REPLY TO
ATTENTION OF

DAMO-FMS 19 March 2014

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: AFMS Policy Letter #7 – Personally Identifiable Information (PII) Incident Reporting and Notification Procedures

1. References.

a. DoD 5400.11-R, DoD Privacy Program, 14 May 2007.

b. Message, HQDA, 261826Z July 2007, subject: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures.

c. DoD Memorandum, 21 September 2007, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII).

d. ALARACT 050/2009, Personally Identifiable Information (PII) Incident Reporting and Notification Procedures, 26 February 2009.

e. ALARACT 187/2010, Protection of Personally Identifiable Information (PII) on Networked Copiers, Printers and other Networked Information Technology (IT) Devices 9 June 2010.

2. Purpose. This policy prescribes the AFMS personnel responsibilities and procedures for reporting and notification of suspected or actual loss of PII.

3. Proponent. The proponent for this policy is the AFMS Director of Information Technolgy.

4. Policy.

a. The AFMS Director of IT is the primary point of contact (POC) for overseeing and managing the PII incident notification and reporting process.

b. Personally Identifiable Information (PII) is all information which can be used by any person to distinguish, trace, or identify another individual. One or two pieces of information can be combined with other information to compromise someone's identity even if the individual pieces of that information seem harmless. This information can be in hardcopy (paper copy files) or electronic format, stored on personal computers, laptops, printers, copiers, networked IT devices and personal electronic devices, and found within databases. This includes, but is not limited to, education records, financial transactions, employment history, criminal records, and medical files.

c. You are the first line of defense in protecting your Personally Identifiable Information.
Information that could be considered PII includes: private phone number, date and place of birth, mother's maiden name and names of family members, financial information, payroll data, banking accounts, and credit/debit card information. Additional PII also includes sensitive and private data related to health, education, medical conditions, private relationships, and marital status. It is not possible to identify all types of personal sensitive information which may accumulate in unit locations or activities.

d. Elements where the government controls when and how they are issued and used about the DoD employee are not considered Personally Identifiable Information. Examples include: Military Rank, Civilian Grade, Official government E-mail address, Official duty location, Duty phone number, Duty title.

e. To protect PII treat it as FOUO. Refrain from storing PII on disks (CDs, USB flash drives, memory sticks, flashcards, etc...) unless the material is encrypted. Government PII should never be stored on personally-owned notebooks, desktops, flash drives, etc. Mark all government provided data storage equipment containing PII records appropriately: "For Official Use Only (FOUO) - Privacy Act Data." Cover or place PII documents in an out-of-sight location when those without an official need to know enter the work space. Remove DoD Common Access Cards (CAC) from their computer before stepping away from the work area, even for brief periods, to ensure protection of PII. Store PII to ensure no unauthorized access during non-duty hours. PII should be stored in a locked desk, file cabinet, bookcase, or office that is not accessible.

f. Most networked copiers, printers and other networked Information Technology devices (both Classified and Unclassified) contain computer hard drives that store images of each document that has been reproduced scanned or sent by the machine. This condition presents a serious vulnerability if the networked devices are disposed of, resold, or sent out for repair with the computer hard drives intact because every document processed or reproduced by the machine could be recreated from images on the machines internal hard drive. Special steps should be taken to ensure removal of the drive or use of DOD approved data cleansing software is performed before removal of the networked IT device from a government facility.

g. All AFMS personnel (Soldiers, civilians and contractors) must complete annual web-based mandatory training on protecting Personally Identifiable Information provided by following the instructions in enclosure 3.

h. A breach or compromised incident occurs when PII is suspected or confirmed as lost, stolen, or is otherwise available to individuals without an official need to know. This includes, but is not limited to, posting PII on publicly accessible web sites, sending PII via electronic mail (e-mail) to unauthorized recipients, providing hard copies of PII to individuals without a need to know, loss of electronic devices storing PII, failing to dispose of hard copies of PII by burning or shredding, using PII for unofficial business, and all other unauthorized access to PII.

i. All suspected or actual loss, theft, or compromise of PII will be reported as indicated below. The enclosed PII Response Checklist/Risk Assessment Model can be used as a reference when reporting a PII incident.

j. Stop collecting immediately any category or item of personal information for which retention is no longer justified. Also delete this information from existing records, when feasible.

k. Do not destroy any records that must be retained in accordance with disposal.

5. Responsibilities and Procedures for PII Incident Reporting.

a. The individual and/or activity discovering an actual or suspected breach/compromise of PII will:

(1) Report the incident immediately to his or her first line supervisor and the Director of Information Technology

(2) Within 1 hour:

(a) Complete and submit the US Computer Emergency Readiness Team (US-CERT) report located at https://forms.us-cert.gov/report/. Scan the US-CERT summary report into a Portable Document Format (PDF) file for subsequent reporting and use the US-CERT tracking number in the subject line of all associated correspondence. If computer access is not available, PII incidents can be reported to the US CERT at (703) 235-5110.

(b) E-mail the US-CERT summary, along with a brief synopsis, point of contact, and contact information to:

1. AFMS Information Assurance Security Manager kurt.w.speed.ctr@mail.mil

2. Regional Computer Emergency Readiness Team at RCERT-CONUS@netcom.army.mil (if an incident involves the possible compromise of Army networks).

3. Fort Belvoir Network Enterprise Center POC: Mr. James Harvey at james.e.harvey14.ctr@mail.mil

(3) Within 4 hours: Submit an Executive Summary (EXSUM), as required by reference 1a, to the AFMS IASO, at email listed above. The EXSUM should be reviewed and approved by the supervisory chain of the individual or activity discovering the actual or suspected breach.

b. AFMS Director of Information Technology will:

(1) Review EXSUMs from the individual or activity discovering the suspected or actual breach and forward to the AFMS Deputy Commandant.

(2) Distribute copies of the US-CERT and the summary synopsis to appropriate parties as needed.

(3) Maintain and report PII incident statistics.

(4) Monitor PII incident reporting to ensure compliance with this policy memorandum.

(5) Within 24 hours submit a report to the Headquarters, Department of the Army, Freedom of Information Act/Privacy Act (FOIA/PA) Office. The online report and submission guidelines are located at https://www.rmda.army.mil/ORGANIZATION/PA-GUIDANCE.SHTML.

c. The AFMS Director of Operations will:

(1) Within 10 days: Recommend the management level for notifying individuals affected by the PII disclosure. Notification will come from a management level sufficient to reassure impacted individuals of the seriousness of the event and of the associated government response. A risk determination will be made in accordance with PII Response Checklist/Risk Assessment Model (enclosure 1).

(2) Alert the affected individuals as soon as possible, but not later than 10 days after the suspected or actual breach/compromise is discovered. The notice to the individual, at a minimum, will address the type of PII data compromised, facts and circumstances surrounding the compromise, protective actions being performed by the agency, and protective actions the individual can take to mitigate potential harm. Sample notification letters are available at https://www.rmda.army.mil/privacy/docs/SampleNotificationLetter.pdf. If the organization cannot readily identify the affected individuals, a generalized notice to the potentially affected population will be published. This general notice may be posted on the organization's web site, local newspaper, or other publicly accessible media.

6. POC for this action is Mr. Kurt Speed, Director of Information Technology, kurt.w.speed.ctr@mail.mil or 703-805-2372.

Albert L Benson

ALBERT L. BENSON
LTC, LG
Deputy Commandant, AFMS

Encls
1. Sample Executive Summary
2. DoD Risk Assessment Model
3. DISA Web based PII Training

Sample Executive Summary (EXSUM)

AFMS Information Assurance (IA) PII Incident Checklist/Risk Assessment Model

Summary: Procedures and requirements for reporting compromise of PII.

Goal: Enable AFMS Personnel to successfully manage a PII compromise.

References:

a. Office of Management and Budget (OMB) Memorandum, 22 May 07, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

b. Department of Defense (DOD) Directive 5400.11, 8 May 07, subject: DOD Privacy Program.

c. DOD Directive 5400.11-R, 14 May 07, subject: DOD Privacy Program.

d. DOD Policy, 18 Aug 06, subject: DOD Guidance on Protecting Personally Identifiable Information (PII).

e. DOD Memorandum, 15 Jul 05, subject: Notifying Individuals When Personal Information is Lost, Stolen, or Compromised.

f. DOD Directive 1000.25, 19 Jul 04, subject: DOD Personnel Identity Protection (PIP) Program. Program.

General Instructions:

All PII incidents must be dealt with in a rapid manner by the individual or organization that detects the compromise. The role of the Director of Information Technology is to ensure proper procedures are followed and the users or data owners understand the mandatory reporting requirements. Propose any procedural changes to the Director of Information Technology.

Procedures:

1. Ensure the party discovering the compromise of PII records/documents the who, what, when, where, how and why associated with the breach of information. In the event of loss or theft of information systems or media, direct immediate contact and reporting to IASO. The DOD Risk Assessment Model is attached for reference when determining the severity of a PII compromise.

2. Within 1 hour: Complete and submit the US Computer Emergency Readiness Team (US-CERT) report located at https://forms.us-cert.gov/report/. Scan the US-CERT summary report into a pdf. file for subsequent reporting and use the US-CERT tracking number in the subject line of all associated correspondence. If computer access in not available, PII incidents can be reported to the US CERT at (703) 235-5110.

3. Within 1 hour: E-mail the US-CERT summary, along with a brief synopsis, point of contact, and contact information to:

(a) AFMS Information Assurance Support Officer (IASO) at kurt.w.speed.ctr@mail.mil

(b) Regional Computer Emergency Readiness Team at RCERT-CONUS@netcom.army.mil (if an incident involves the possible compromise of Army networks).

(c) Fort Belvoir Network Enterprise Center POC: Mr. James Harvey at james.e.harvey14.ctr@mail.mil

4. Within 4 hours: Submit an Executive Summary (EXSUM), as required by reference 1a, to the AFMS IASO, at email listed above. The EXSUM should be reviewed and approved by the supervisory chain of the individual or activity discovering the actual or suspected breach.

AFMS Information Assurance (IA) PII Incident Checklist/Risk Assessment Model

UNCLASSIFIED

EXECUTIVE SUMMARY

10 July 20xx

(U) COMPROMISE OF PERSONALLY IDENTIFIABLE INFORMATION (PII) (U) (MCCS-XYZ) On 2 JUL 20xx, twelve laptop computers were stolen from the AFMS facility, Building 247 on Fort Belvoir, VA. All computers contained class rosters containing full name, SSN, mailing address, home telephone, date of birth, official photo and Government credit card account information. This incident was reported to the AFMS Director of Information Technology upon discovery. The Criminal Investigation Division has opened an investigation and initial notification to all affected students is ongoing. Incident has been reported to the United States Computer Emergency Response Team (US-CERT), reference #XXXX00.

MAJ Promotable/AFRC-XYZ/(210) 221-xxxx

APPROVED BY: COL BOSS

UNCLASSIFIED

DoD Risk Assessment Model

No.	Factor	Risk Determination	Low Moderate High	**Comments:** All breaches of PII, whether actual or suspected, require notification to US-CERT. Low and moderate risk/harm determinations and the decision whether notification of individuals is made, rests with the Head of the DoD Component where the breach occurred. All determinations of high risk or harm require notifications.
1.	What is the nature of the data elements breached? What PII was involved?			
	a. Name only	Low		Consideration needs to be given to unique names; those where one or only a few in the population may have or those that could readily identify an individual, i.e., public figure.
	b. Name plus 1 or more personal identifier (not SSN, Medical or Financial)	Moderate		Additional identifiers include date and place of birth, mother's maiden name, biometric record and any other information that can be linked or is linkable to an individual.
	c. SSN	High		
	d. Name plus SSN	High		
	e. Name plus Medical or Financial data	High		
2.	Number of Individuals Affected			The number of individuals involved is a determining factor in how notifications are made, not whether they are made.
3.	What is the likelihood the information is accessible and usable? What level of protection is applied to this information?			
	a. Encryption (FIPS 140-2)	Low		
	b. Password	Moderate/High		Moderate/High determined in relationship to category of data in No. 1.
	c. None	High		
4.	Likelihood the Breach May Lead to Harm	High/Moderate/Low		Determining likelihood depends on the manner of the breach and the type(s) of data involved.
5.	Ability of the Agency to Mitigate the Risk of Harm			
	a. Loss	High		Evidence exists that PII has been lost; no longer under DOD control.
	b. Theft	High		Evidence shows that PII has been stolen and could possibly be used to commit ID theft.
	c. Compromise			
	(1) Compromise with-in DOD control	Low High		No evidence of malicious intent or possibility of malicious intent.
	(2) Compromise beyond DOD control	High		Possibility that PII could be used with malicious intent or to commit ID theft.

DISA Web Based PII Training

To access the Personally Identifiable Information training course: http://iase.disa.mil/eta/piiv2/launchpage.htm. **Click the launch button to access the course. After completion of the course print certificate and forward to the AFMS Director of Information Technology.**

Encl 3